NIST Activities on IPv6

Stephen Nightingale and Doug Montgomery

NIST-ITL IPv6 Project

For: ISPAB March 22nd, 2007

Draft USGIPv6 – v 1.0

- **Public Review**: February 1, 2007.
- **Closed**: March 2, 2007.
- 400+ Public Comments received
- 33 Individuals and Organizations commented.
- Comments received include Policy as well as Technical concerns.

Outline of the Talk

- (1) A Walk Through the Profile.
- (2) Differences from other Profiles (IETF, DoD, IPv6ready).
- (3) Major Comments Received.
- (4) Other Procedural Consequences.
- (5) Testing Arrangements.
- (6) Harmonization?

Walkthrough: Purpose and Scope

- **NIST SP 500-267**
  - Recommended acquisition profile from NIST for agencies seeking operational deployment of IPv6 technologies.
    - **Policy Free** – other USG and Agency specific policies may use this as a basis for further definition.
    - **Minimal Interoperability IPv6 subset for common devices and expected services.**
      - Defining the low bar to provide expected functionality, achieve interoperability, insure security and protect potentially significant resource investments.
      - In some areas our low bar is higher than current industry norms.
      - Not trying to specify everything that might be in a box; instead, what we think must be in a box.
    - **Expected that Agencies will add additional requirements as needed**.
      - Things missing from our profile are by definition "optional" and may be added by agencies/programs as needed.
    - **Focus on IPv6 Data Plane**
      - Get to viable IPv6 data plane first, then go for IPv6 only devices.
    - **Defines USGIPv6-v1.0 compliant Hosts and Routers**.
      - Expected to put a testing program in place to verify compliance to the profile.

Walkthrough:Goals and Objectives

- **Support OMB/GSA policies**.
  - **Provide a basis** through which OMB and GSA can further refine either emerging acquisition and deployment polices.
    - Avoid policy confusion – allow policy sources to define "USG IPv6 Capable" and FAR in terms of (our) profile.
    - Fill in the technical pieces necessary to support these policies and their time frames.
      - E.g. provide interim specification of Network Protection Devices (firewalls and IDS systems) vital to ensure the security of Federal IT systems under OMB deployment strategy.
- **Leverage DoD/IETF/Industry efforts**.
  - DISR, IETF Node requirements, IPv6Ready, NSA, ICSA profiles and testing programs carefully analyzed.
    - Considered existing content capabilities, governance and timing issues.
  - USGv6V1.0 is a synthesis/intersection of these efforts mixed with USG specific requirements.
  - Long term goal is to get to the point where a distinct USG profile/testing program is unnecessary.

Walkthrough:Profile Overview

- **Scope and Application**
  - **Strategic planning document** to guide acquisition of IPv6 technologies for large scale, operational deployments.
  - Defines minimal *low bar* of capabilities to:
    - Insure Interoperability.
    - Enable secure operation.
    - Protect early investments.
  - **Basis for further refinement and definition**.
    - Agency/mission specific technical requirements.
    - Acquisition/deployment policies.
- **USGIPv6-V1 Compliant**
  - Provides technical basis for product testing and certification program.

Walkthrough:Profile Categorization

- **Sub profiles for 3 types of device**.
    - Host Profile.
    - Router Profile.
    - Network Protection Device Profile.
- **12 Functional Categories of Capabilities**.
    - 6.1 Base
    - 6.2 Routing
    - 6.3 Quality of Service
    - 6.4 Transition
    - 6.5 Link Technology
    - 6.6 Addressing
    - 6.7 IPsec
    - 6.8 Application Environment
    - 6.9 Network Management
    - 6.10 Multicasting
    - 6.11 Mobility
    - 6.12 Network Protection Devices
        - Sources of Requirements.
        - Common requirements for NPDs.
        - Firewall requirements.
        - Intrusion detection and prevention system requirements.

Walkthrough:The Spreadsheet

- *See pages 30-40 of the profile.*

Differences from other Profiles

Profile	Dev	FC	Rev	IPsec 2401	IPsec 4301	AH
IETF	2	No	No	obs	refer	agno
DISR	6	Yes	Part	M	M	Yes
V6Ready	2	No	Yes	-	-	No
USG	3	Yes	Part	M	S+	No

Major Comments Received

- Policy
- Security
- Product Classes
- Network Protection
- Routing Protocols
- Calls for Harmonization
- Applications
- Crypto Generated Addresses
- IPv4-IPv6 Translation

Comments: Policy

- **From Agencies and from Industry**:
  - What is the Profile's applicability, i.e. what 'Must' agencies do or not do and when?
  - Does NIST have any plans to produce a 'Classified' Profile?

Comments: Security

- Mandate AH (or not).
- Mandate RFC 4301 and deprecate 2401 (or not).

Comments: Product Classes

- **Use DoD DISRs 6 product categories**.
  - Do not mandate 'full' IPv6 compliance for certain devices, such as IP phones.
- **Or, Current 3 categories are okay**.
- **Split the Router** category into finer gradations.

Comments: Network Protection

- **Publish this as a separate Specification**.
  - It "doesn't belong" in an IPv6 profile.
- **Advance** it to an **RFC** in the *IETF*.
- **Beef up** the MUST/MAY language to **RFC 2115.**

Comments: Routing Protocols

- **More flexibility required for Interior Gateways**:
  - Do not require only OSPF.
  - Optionally allow one of OSPF, RIP, IS-IS, or others.
  - Allow BGP as an optional Interior Routing protocol.

Comments: Calls for Harmonization

- Harmonize with the DoD DISR profile.

Comments: Applications

- Calls to add a **DNS** specification.
- Calls to add **Applications**.

Comments: Crypto-Generated Addresses

- Crypto Generated Addresses.

- Or, Do not require Crypto Generated addresses because there is IPR restricting their use.

Comments: v4-v6 Translation

- Calls to include IPv4-IPv6 Translation as a transition method.

Other Procedural Consequences

- **OMB/GSA** are in the throes of hatching a **FAR** clause that will depend on the NIST profile and Testing recommendations.

- Calls for *Industry interaction* may lead to a government organized 'Industry Day'.

- There is need for policy to include *Revision Management* beyond a June 2008 'Red Flag' day.

Testing Arrangements

- **Existing Analysis**
  - DoD JITC
  - IOL/IPv6 ready
  - ICSA
  - Commercial Tool Industry
- **What We Need**
  - Interoperability
  - Conformance
  - Approved Products List
- **Steps**
  - Public Meeting.
  - NIST recommendations to OMB.
  - Establishment of a Testing program and APL.

Harmonization

- **Initial DOD Profile WG group reaction**: "*there is very substantial overlap*".
- **IPv6Ready reaction** is *positive*.
- But **USG** now makes it 3.
- **De facto compliance** Today is to DOD or IPv6Ready.
- **USG compliance** not likely before 2Q/3Q 2008.
- **Harmonization efforts** with IPv6Ready and DoD after this Rev. should lead to 2 or 1 remaining profile.
  - (Optimistically) harmonized profile applicability by 18m – 2yrs after USG applicability.
- **Is there a need** for Incremental profiles involving IPv6 Applications?